

Claims:

I claim:

1. A computer file containing digital data wherein authentication information is encoded in the filename of said computer file at a predetermined position or using delimiters.

2. A method for encoding authentication information in the filename of a computer file containing digital data, said method comprising the steps of:

computing a digital signature of the computer file using a private key of a sender; and,

encoding said computed digital signature in a filename of said computer file at a predetermined position or using delimiters.

3. The method of claim 2, wherein the step of encoding said computed digital signature includes the step of adding said computed digital signature in the filename just before the file extension, said computed digital signature having a fixed size.

4. The method of claim 2, wherein the step of computing a digital signature is based on a symmetric or public-key algorithm.

5. The method of claim 2, wherein the step of computing a digital signature includes the steps of: computing a hash value of said computer file; and computing a digital signature of the computed hash value using the private key of the sender.

6. The method of claim 5, wherein said step of computing a hash value uses a Secure Hash Algorithm or a Message-Digest-5 algorithm.
7. The method of claim 2, further comprising the step of applying said method to files attached or linked to the computer file.
8. Apparatus comprising means adapted for carrying out the method according to claim 2.
9. A computer readable medium comprising program instructions for carrying out the method according to claim 2.
10. A method for authenticating a computer file having a filename comprising authentication information, said method comprising the steps of:

extracting said authentication information from the filename of the computer file at a predetermined position or using delimiters;

recovering an encoded hash value of the computer file by using a public key of a sender of the computer file and the extracted authentication information;

computing a hash value of said computer file using a hash function used by the sender to generate the encoded authentication information;

comparing the encoded and the computed hash values; and,

if the encoded and the computed hash values are identical, processing the computer file, else, if the encoded and the computed hash values are different, rejecting the computer file.

11. The method of claim 10, further comprising the step of applying said method to files attached or linked to the computer file.

12. Apparatus comprising means adapted for carrying out the method according to claim 10.

13. A computer readable medium comprising program instructions for carrying out the method according to claim 10.